



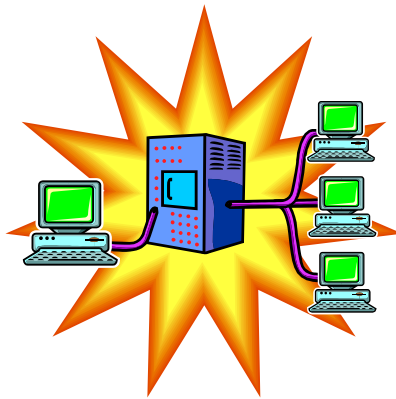
DoD PKI

Server Certificate

Enabling For

Microsoft Internet Information Server 5.0

Step 1: Generating a Key Pair and Requesting a Certificate



PK-Enabling For Microsoft Internet Information Server (IIS 5.0)

Step 1: Generating a Key Pair and Requesting a Certificate

This Document details how to generate a PKI key pair and request a server certificate using Microsoft Internet Information Server 5.0. It covers step 1 of a 2-step process. “Server Certificate Enabling for Microsoft Internet Information Server 5.0: Step 2: Obtaining/Installing a PKI Certificate” is a follow-up document. It details how to obtain and install a PKI server certificate as well as how to make the web server secure (https).

Step 1: Generating a Key Pair and Requesting a Certificate

Step 1 – Generating a Key Pair.	Page 3
Step 2 – Requesting a Certificate.	Page 12
Step 3 – Approval Notification.	Page 15

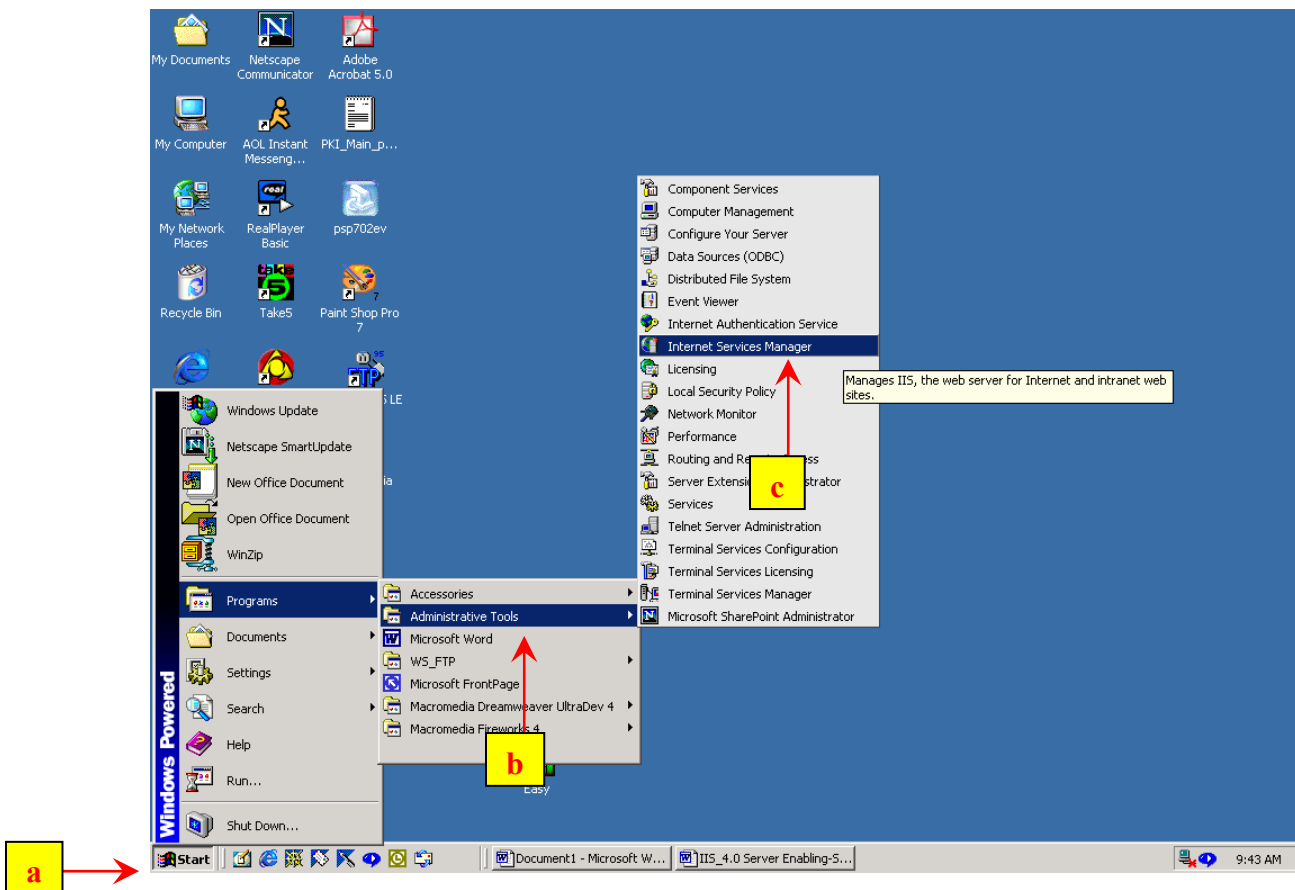
PK-Enabling For Microsoft Internet Information Server (IIS 5.0)

****The following must be installed before attempting to install DoD certificates onto your server. ALL SOFTWARE LISTED BELOW MUST BE 128-BIT.**

1. Windows 2000 Server
2. Netscape 4.5 or greater
3. IE 5.0 or greater

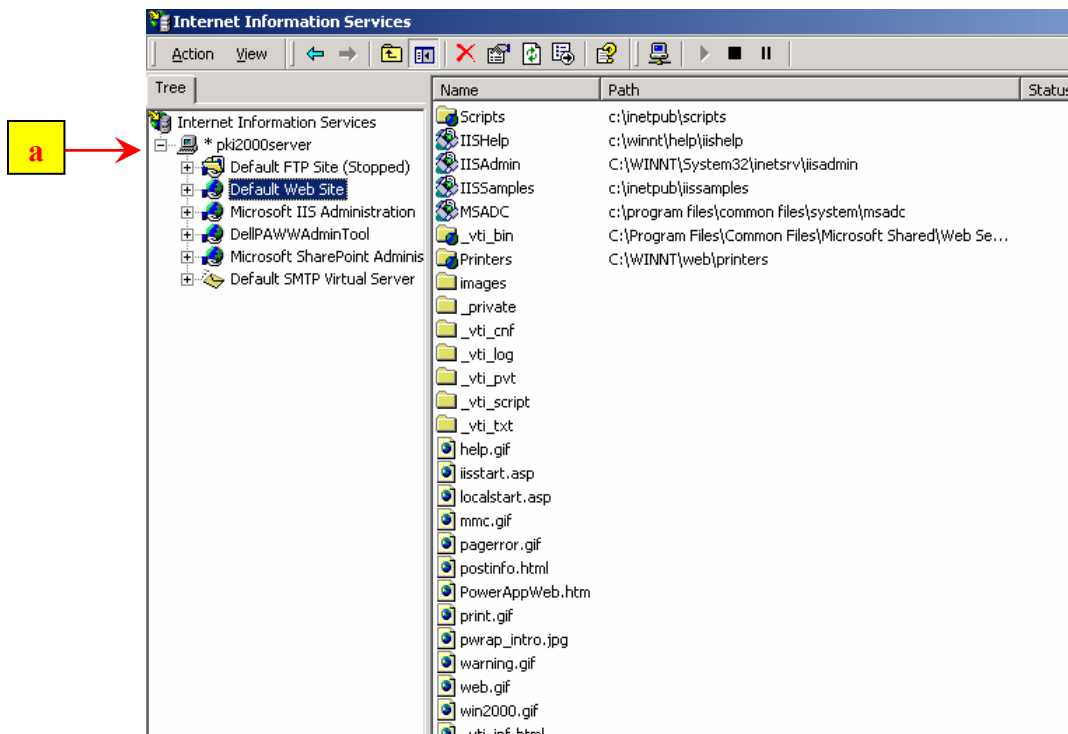
Generating a Key Pair

- 1) Generating a Key File.
 - a) Click **Start, Programs.**
 - b) **Administrative Tools.**
 - c) **Internet Service Manager.**



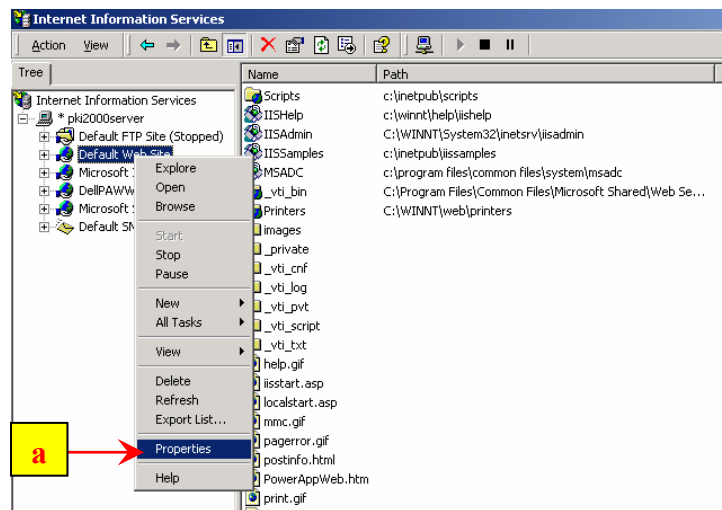
2) Expand the Server

a) Click on * *your server name*.

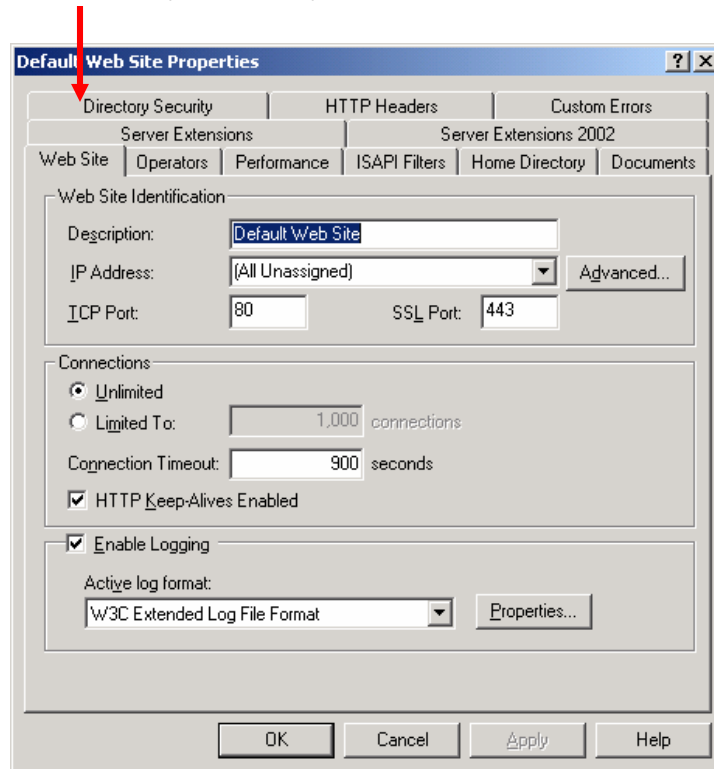


3) Open the Properties Dialog Box.

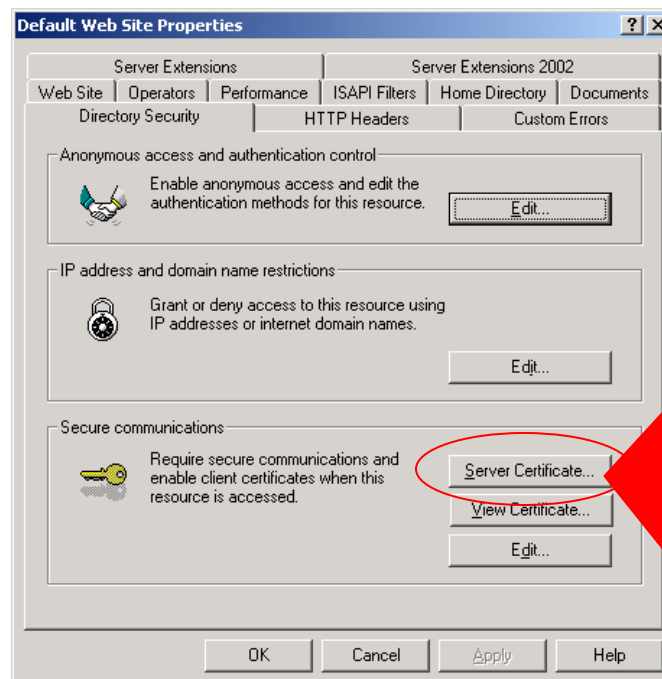
a) Right click on the desired web site and choose **Properties**. The Administrative Web Site Properties dialog box appears.



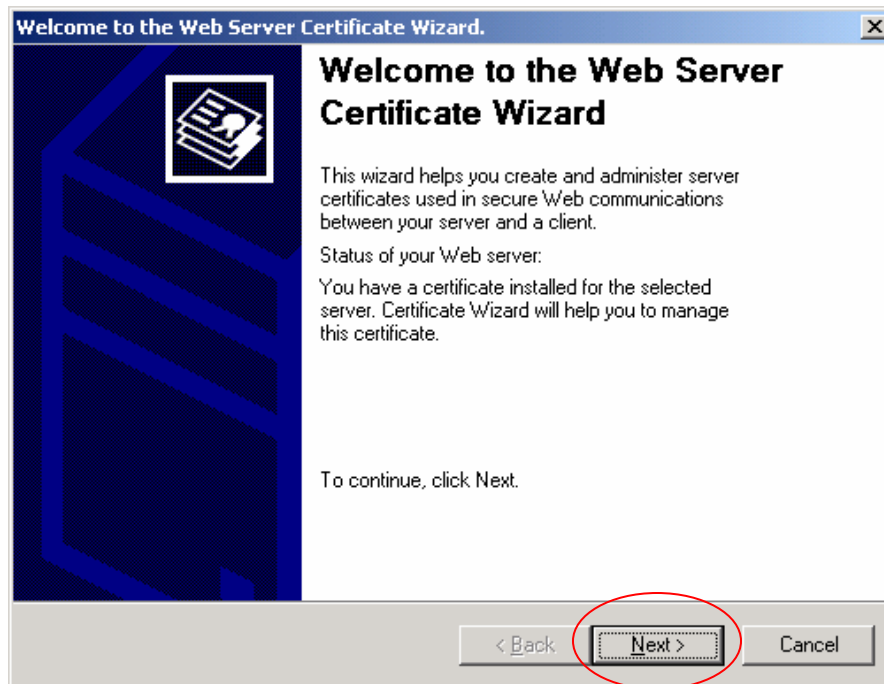
4) Click on the **Directory Security Tab**.



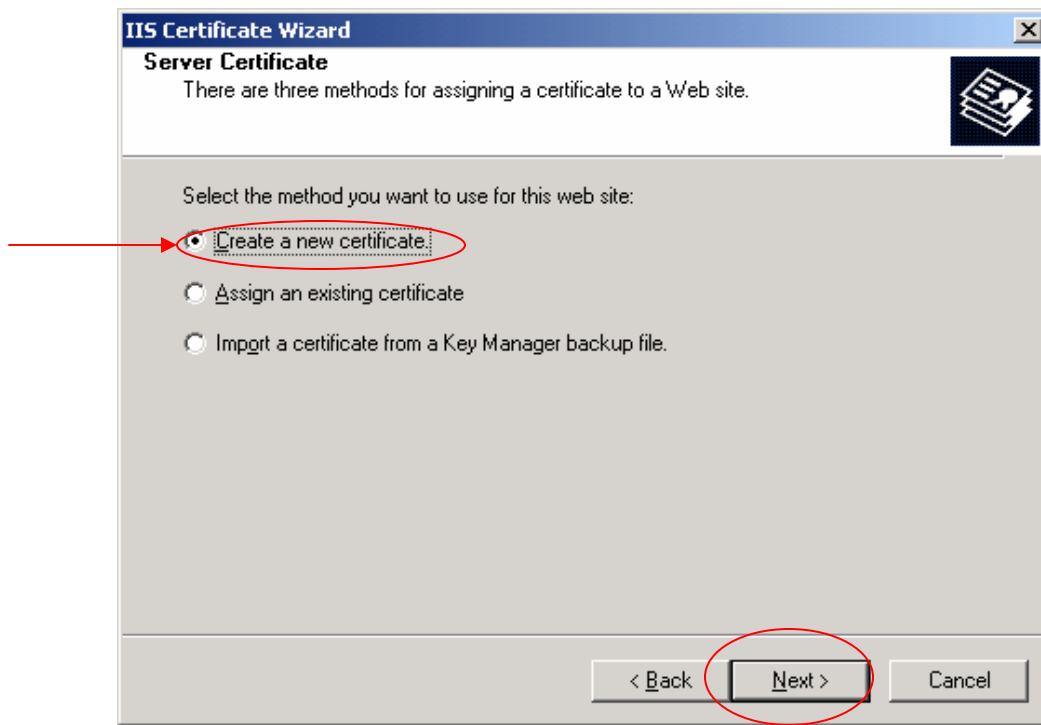
5) Under Secure Communications, click **Server Certificate**



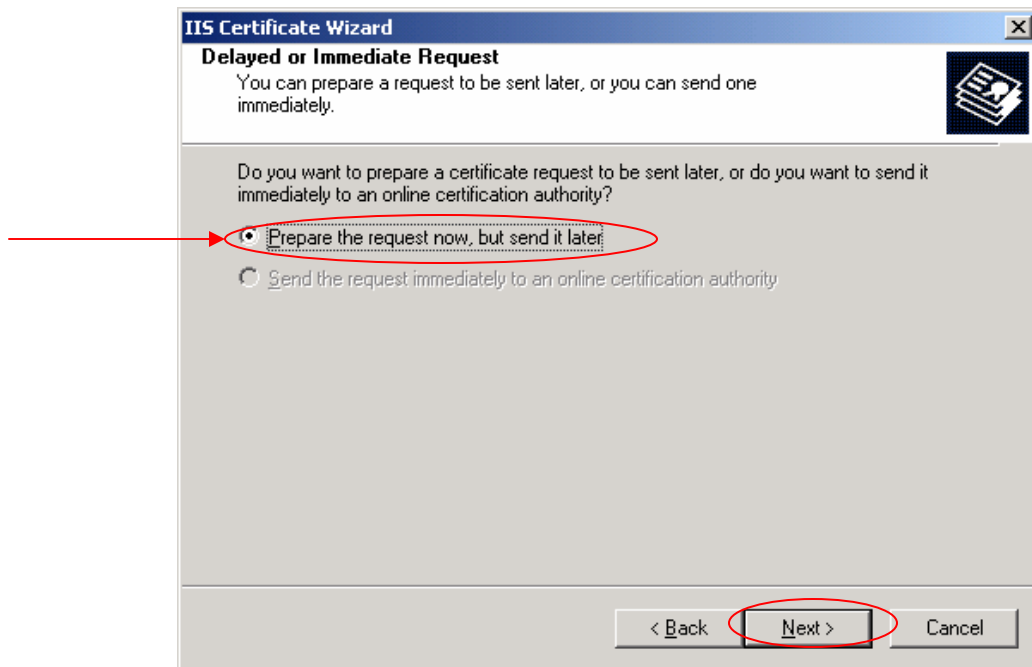
6) Click **Next**.



7) Confirm that the **Create a New Certificate** button is selected and then click **Next**.



- 8) Click the **Prepare the request now, but send it later** button and then click **Next**.



- 9) Fill in the **Name** field with the exact url you type to access your website. In the **Bit Length** field change your selection to **1024**. Click **Next**.



10) In the Organizational field, type **U.S. Government**, and in the Organizational Unit box, type **USN OU=PKI OU=DoD**. Click **Next**.

*****NOTE:** The text is case-sensitive. There is a space after the letters **U.S.** and the word **Government**. There is also a space after **USN** and the letters **OU=PKI**. There is another space after the letters **PKI** and the letters **OU=DoD**. The letter “o” in **DoD** is lowercase. There is no period after the **DoD**.

IIS Certificate Wizard

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization:

U.S. Government

Organizational unit:

USN, ou=PKI, ou=DoD

< Back Next > Cancel

11) In the **Common Name** text box, type the domain name of your web site, for example, www.basename.navy.mil and then click **Next**. The **Common Name** is the fully qualified domain name (FQDN) of the server that the certificate will be installed on.

IIS Certificate Wizard

Your Site's Common Name

Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:

www.servername.mil

< Back Next > Cancel

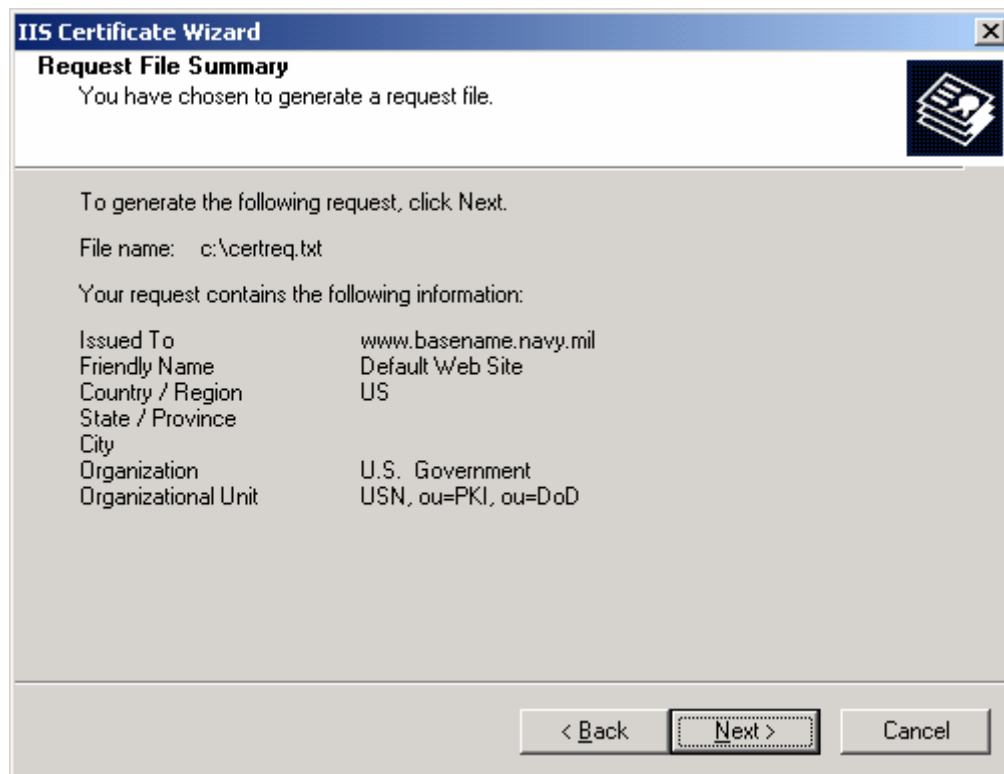
- 12) In the **Country/Region** box, type **US** (United States). Normally, this should be the default.
- 13) In the **State/province** box, press **Spacebar**. To move to the **City/locality** field, press **TAB** or click the **City/locality** box.
- 14) In the **City/locality** box, press **Spacebar**.
- 15) Click **Next**.

The screenshot shows the 'IIS Certificate Wizard' window at the 'Geographical Information' step. The window title is 'IIS Certificate Wizard' and the subtitle is 'Geographical Information'. Below the subtitle, it says 'The certification authority requires the following geographical information.' There are three input fields: 'Country/Region:' with a dropdown menu showing 'US (United States)', 'State/province:', and 'City/locality:'. Red arrows point to these fields from yellow boxes labeled 12, 13, and 14 respectively. Below the fields, a note states: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A red arrow points to the 'Next >' button from a yellow box labeled 15. A yellow note box on the right says: 'Note: State/Province and City/Locality must be blank, but IIS 5.0 doesn't allow for blanks so for each field, press the spacebar once.'

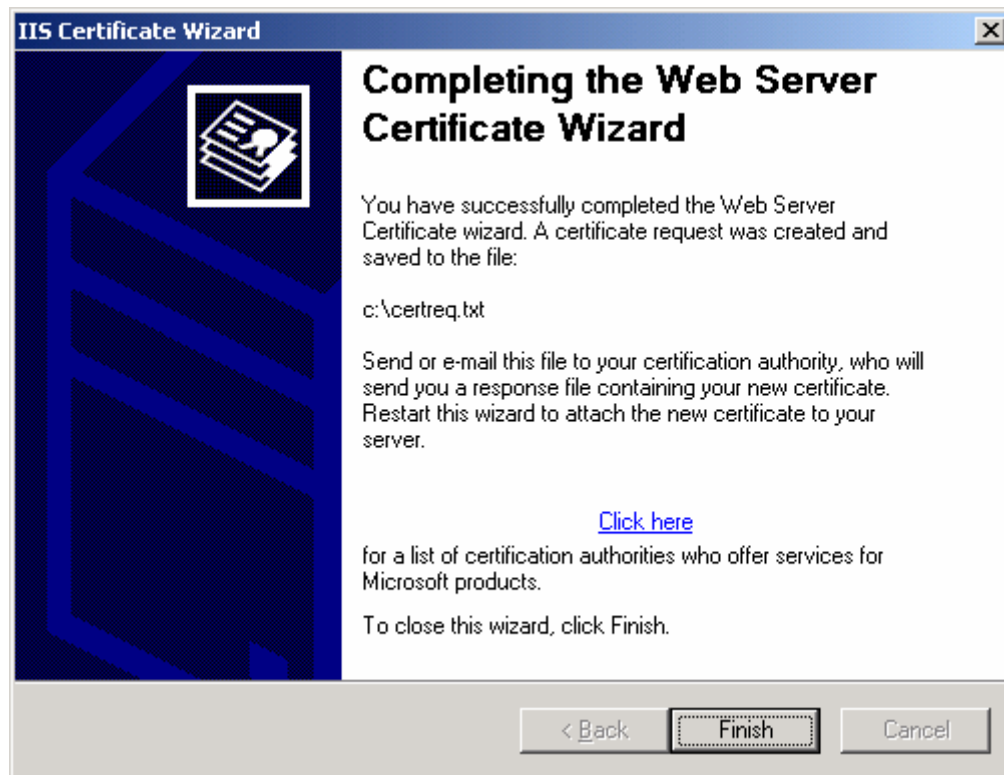
- 16) In the **File name** box, enter a file name. Remember the folder where the file is save. You may also click **Browse** to locate the desired folder. The file name should have a **.txt** extension and is saved in a text format. Click **Next**.

The screenshot shows the 'IIS Certificate Wizard' window at the 'Certificate Request File Name' step. The window title is 'IIS Certificate Wizard' and the subtitle is 'Certificate Request File Name'. Below the subtitle, it says 'Your certificate request is saved as a text file with the file name you specify.' There is a text input field labeled 'File name:' with the text 'c:\certreq.txt' entered. A red arrow points to this field. To the right of the field is a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 17) The **Request File Summary** screen appears. Read through the summary information on the screen.
- If changes need to be made, click **Back** as many screens as necessary to make changes.
 - After making the changes, click **Next** as many times as needed to get back to this screen.
 - Click **Next** to display the **Completing the Web Certificate Wizard** screen.



- 18) **The Completing the Web Server Certificate Wizard Screen** informs you that the certificate request has been successfully completed. This screen displays the file folder and the file name of the certificate request. Click **Finish**.



- 19) You will now need to open a web browser to communicate with the *Certificate Authority* server to submit your certificate request. You will need to open **Windows Notepad** to copy and paste information from the clipboard during this operation.

Requesting a Certificate

After generating a request for a web server certificate, you will submit the request to the **DoD Certificate Authority**. You may use either *Netscape Navigator 4.05* or newer or *Internet Explorer v5.01* or newer.

- 1) Open your browser and type the URL <https://ca-3.c3pki.chamb.disa.mil> in the address box. The **Manual User Enrollment** page will display.
- 2) Click on **Manual** under Server Enrollment.

Manual User Enrollment

Use this form to submit a request for a personal certificate. After you click the Submit button, your request will be submitted to an issuing agent for approval. When an issuing agent has approved your request you will receive the certificate in email, along with instructions for installing it.

Important: Be sure to request your certificate on the same computer on which you plan to use the certificate.

User's Identity
Enter values for the fields you want to have in your certificate. Your site may require you to fill in certain fields.

Full name:
Login name:
Email address:
Organization unit:
Organization:
Country:

Contact Information
Enter an email address or phone number at which you can be contacted regarding this request.

3) The Server Certificate Enrollment (for Server Administrators) will display.

Netscape Certificate Management System

Certificate Manager

Enrollment Renewal Revocation Retrieval

User Enrollment

Manual

Directory Based

Directory and Pin Based

Server Enrollment

Manual

Registration Manager Enrollment

Manual

Certificate Manager Enrollment

Manual

Server Certificate Enrollment (for Server Administrators)

Use this form to submit a request for a server certificate. You must submit a PKCS #10 request. If you have a Netscape server, create a PKCS#10 request by using the Netscape Administration Server instance associated with the server for which you are requesting the certificate. In the Netscape Administration Server forms, choose Encryption, then Request Server Certificate.

If you are not using a Netscape server, follow the appropriate steps to generate a PKCS #10 request with the server you have.

After you click the Submit button, your request will be submitted to an issuing agent for approval. You will receive the certificate in email when it has been approved.

PKCS #10 Request

Paste the PKCS #10 request into this text area.

Server Administrator Contact Information

Name:

Email:

4) Use **Notepad** to open the certificate request (e.g., certreq.txt) file you generated from the web server.

*****NOTE:** Keep the *Server Certificate Enrollment* window displayed in the browser. You will need to copy the certificate information from Notepad file into this browser screen.

Highlight the text including **BEGIN NEW CERTIFICATE REQUEST** header and **END NEW CERTIFICATE REQUEST** trailer with all dashes. To copy this text to the Windows Clipboard, right-click the selected text, and from the shortcut menu, click **Copy**.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDHjCCAocCAQAwgYgXhJACBgnVBAMTFxd3dy51YXN1bmFtZS5uYXZ5Lm1pbDE
MAoGA1UECXM0VFNOMQwwCgYDVQQLLEwNQ50kxDDAKBgNVBASTA0RVRDEZMBcGA1UE
ChMQVS5TLiAgR292ZXJubWVudDEJMAcGA1UEBxMAMQkwBwYDVQQIEwAxczA1BgNV
BAYTA1VTMIGFMA0GCsgGSIb3DQEBAQUAA4GNADCBiQKBgQC/1dVS98B4ZZ/6j4Vc
dewh+Lo/L8pkBNFgvKfwGngTI4re19Excjm1JmVTV8gx713Hs3t+Qmx7UHWd6AEX
4aP/ez1pHfkG7B1gqughQpjhzygngR0S31Fvz7r8TtSwouZ16GG2C05d8UsAhQpW
e7e1R22ug6tE28pxqtKY+1fEkQIDAQABoIIBUzAaBggorBgEEAYI3DQIDMQwwCjUu
MC4yMTk1LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYDVROPAQH/BAQDAGTWMBMGA1Ud
JQQMMAoGCCSGAQUFBwMBMIH9BggorBgEEAYI3DQICMYHUMIHrAgEBH1OATQBpAGMA
jCBVAHMAbWBMhAQAIABSAFMAQQAGAFMAQwBoAGEAbgBUAGUAbAAgAEMAQGB5AHAA
dABvAGCAGCBhAHAAaABPAGMAIABQAHIAbwB2AGkAZAB1AHIDgykA1uYPzZPpbLgC
wYnXoNex2gs6nuI4osrWHlQQKcs67Vjc1hEL1nt3hBb9B1r7I0Bs1/1guzvZFTZn
C1bmENULRg17bhExtg+nuovzPcJhMvG7G3DR17Pr17V+egHASQV4dQC2hogghonv
88Jhp9Pwps03t2tqjRoA5ZNRSSJskw8AAAAAADAANBgkqhkiG9w0BAQUFAAOB
GQA0q7SuorSoky1t0+BZS4stSeUT/zX1TIbbo6/1okFOGnu0QJnuhgP0kn1jhmK
4ZwyI1wszF1UwQvug1/otmVWS4v3CMWU14Pex64g/G7BMF7tbtPAezE1hFp77gy1
ocZITvLP0y1X6JBWU9jvh0RTx1wHLCvsbyh7kUCTwrw1A==
-----END NEW CERTIFICATE REQUEST-----
```

- 5) Click the browser window to make it the active window. The **Request a Server Certificate** page should still be displayed. Click in the **PKCS #10 Request** text area as shown in the next page.
- 6) Right-click in the text area, and from the shortcut menu, click **Paste** to copy the certificate request information from the Clipboard into the **Server Certificate Enrollment** form.
- 7) Complete the additional information on this web page. You may need to scroll to see the bottom of the page. Click **Submit Request** to display the **Request Successfully Submitted** screen.

Netscape® Certificate Management System

Certificate Manager

Enrollment / Renewal / Revocation / Retrieval

User Enrollment

Manual / Directory Based / Directory and Pin Based

Server Enrollment

Manual

6

PKCS #10 Request

Paste the PKCS #10 request into this text area.

```
JQQMMaocCCsGAQUFBwMBMIH9BgocBgEEAYI3DQICMYHuMIHrAgEBH1oATOQpAGMA
cgBvAHMabwBmAHQAIABSAFMAQAQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcgB5AHAA
dABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZAB1AHIDgYkAjuYPzZPpbLgC
WYnXoNeX2gS6nuI4osrWH1QQKcS67VJc1hEL1nT3hBb9Blr7IOBsJ/1guZvZFTzn
C1bMeNULRg17bhExTg+nUovzPcJhMvG7G3DR17PrJ7V+egHAsQV4dQC2hOGGhOnv
88JhP9Pwps03t2tqJROa5ZNRRSJSKw8AAAAAADAANBqkqhk1G9wOBAAQUFAAOB
gQA0q7SUorsQky1t0+BZS4stSeUT/zX1TI1bbO6/1okFOGnU0QJNuhqPOkN1jhMk
4zWyI1WszF1uwQVUgl/otmVWS4v3CMWU14Pex64g/G7BMF7tbtPAezE1hFp77gyj
oc27ITv1P0y1X6JBUU9jVhORTx1wHLCVsbYh7kUCtwrW1A==
-----END NEW CERTIFICATE REQUEST-----
```

Server Administrator Contact Information

Name:

Email:

Phone:

Additional Comments

7

- 8) The **Request Successfully Submitted** web page will display.

Netscape® Certificate Management System

Certificate Manager

Enrollment / Renewal / Revocation / Retrieval

User Enrollment

Manual / Directory Based / Directory and Pin Based

Server Enrollment

Request Successfully Submitted

Congratulations, your request has been successfully submitted to the Certificate Manager. Your request will be processed when an authorized agent verifies and validates the information in your request.

Your request ID is 9156.

Your can check on the status of your request with an authorized agent or local administrator by referring to this request ID.

This is your Request ID Number

Print this screen for your records or write down your **request ID #**. Close all open windows or applications at this time.

Approval Notification

Approval Notification.

a. The next step in the Server Certificate Request Process involves sending an email to your LRA identifying by the request ID number produced at the end of the last section that the certificate request is ready for review. The email must contain the following (**everything in bold is to be typed as shown** with the rest of the information being replaced with what is appropriate for each individual server):

Reference Number: xxxx (with xxxx being the request ID number received from the last section)

Host Name: www.sample.navy.mil (this is an example only)

IP Address: 102.21.12.12 (the server's ip address)

Region: East Coast

Base: Base Name

Network System Administrator (NSA): Sgt John Doe

System Owner: SPAWAR

Security Level: SBU (Sensitive But Unclassified)

Applications on Server: Development versions of the following:

- 1) SPAWAR PKI Home Page
- 2) INFOSEC Home Page

Certification Justification/Requirements:

- To enable SSL on the server.
 - a. The LRA/RA, upon receipt of the email, will review the request. If the request was done correctly and is approved, the LRA/RA will send an email that will contain a *Certificate Serial Number (CSN)*. The CSN must be utilized in order to download the certificate. If the request is not approved, the RA will notify the requestor/LRA why.
 - b. If the requestor does not receive anything from the LRA/RA within 1 week after the email was sent, contact the LRA/RA by phone.
 - c. When the email with the CSN has been received, refer to "Server Certificate Enabling for Microsoft Internet Information Server 5.0 Step 2: Obtaining/Installing PKI Server Certificate.